

WHAT IS CLAIMED IS:

1 1. A modular multiplier, capable of processing a first
2 operand and a second operand in relation to a modulus for
3 performing a modular multiplication operation, the performed
4 operation including an instruction, which has an internal
5 multiplication and addition operation with inner recursion
6 and an external multiplication and addition operation, the
7 modular multiplier comprising:

8 a first buffer device for storing the first operand,
9 wherein the first operand is divided into a first plurality
10 of sub-operands with fixed length;

11 a second buffer device for storing the second operand,
12 wherein the second operand is divided into a second
13 plurality of sub-operands with fixed length;

14 a third buffer device for storing the parameter of the
15 modular multiplication operation;

16 a multiplexer device coupled to the first, the second,
17 and the third buffer devices, for choosing a first
18 multiplication operand and a second multiplication operand
19 from the first sub-operand, the second sub-operand, and the
20 parameter according to the required internal and external
21 multiplication/addition operations;

22 a multiplication device coupled to the multiplexer
23 device, for multiplying the first multiplication operand by
24 the second multiplication operand to obtain a product; and

25 an addition device coupled to the multiplication
26 device, for outputting an intermediate result according to
27 the product during the internal multiplication and addition
28 operation and outputting the result of the modular
29 multiplication operation according to the product and the

intermediate result during the external multiplication and addition operation.

2. The modular multiplier of Claim 1, wherein the addition device further comprises:

a first delay component coupled to the multiplication device, for receiving half of the product at the lower-bit portion;

a second delay component coupled to the multiplication device, for receiving half of the product at the higher-bit portion, wherein the second delay component has a multiplication clock more than the first delay component; and

an adder coupled to the first delay component and the second delay component, for receiving intermediate values from the first and second delay components to perform the addition operation.

3. The modular multiplier of Claim 1, further comprising an encryption processor for encrypting a plaintext using an encryption key according to a modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

4. The modular multiplier of Claim 3, further comprising a decryption processor for decrypting a ciphertext using a decryption key according to the modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

13 5. The modular multiplier of Claim 1-, further
14 comprising a smart card having an encryption/decryption
15 processor for encrypting/decrypting internal data, wherein
16 the encryption/decryption processor performs the encryption/
17 decryption using an encryption/decryption key according to a
18 modular exponentiation operation, and the modular
19 exponentiation operation is performed by the multiplier.
20

21 6. A modular multiplier, capable of processing a first
22 operand and a second operand in relation to a modulus for
23 performing a modular multiplication operation, the performed
24 operation including an external loop and an internal loop,
25 the internal loop having an instruction, which has an
26 internal multiplication and addition operation with inner
27 recursion and an external multiplication and addition
28 operation, the modular multiplier comprising:

29 a first buffer device for storing the first operand,
30 wherein the first operand is divided into a first plurality
31 of sub-operands with fixed length, each sub-operand
32 respective to the external loop;

33 a second buffer device for storing the second operand,
34 wherein the second operand is divided into a second
35 plurality of sub-operands with fixed length, each sub-
36 operand respective to the internal loop;

37 a third buffer device for storing a first and a second
38 parameters of the modular multiplication operation;

39 a multiplexer device coupled to the first, the second,
40 and the third buffer devices, for choosing a first
41 multiplication operand and a second multiplication operand,
42 which are selected from one of the two groups, the first
43 sub-operand and parameter and the second sub-operand and

44 parameter according to the required internal and external
45 multiplication/addition operations;

46 a multiplication device coupled to the multiplexer
47 device, for multiplying the first multiplication operand by
48 the second multiplication operand to obtain a product;

49 an addition device coupled to the multiplication
50 device, for outputting an intermediate result according to
51 the product during the internal multiplication and addition
52 operation and outputting the result of the modular
53 multiplication operation according to the product and the
54 intermediate result during the external multiplication and
55 addition operation; and

56 a controller for outputting a control signal to control
57 the multiplexer.

58
59 7. The modular multiplier of Claim 6, wherein the
60 addition device further comprises:

61 a first delay component coupled to the multiplication
62 device, for receiving half of the product at the lower-bit
63 portion;

64 a second delay component coupled to the multiplication
65 device, for receiving half of the product at the higher-bit
66 portion, wherein the second delay component has a
67 multiplication clock more than the first delay component;
68 and

69 an adder coupled to the first delay component and the
70 second delay component, for receiving intermediate values
71 from the first and second delay components to perform the
72 addition operation.

8. The modular multiplier of Claim 6, further comprising an encryption processor for encrypting a plaintext using an encryption key according to a modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

9. The modular multiplier of Claim 8, further comprising a decryption processor for decrypting a ciphertext using a decryption key according to the modular exponentiation operation, wherein the modular exponentiation operation is performed by the modular multiplier.

10. The modular multiplier of Claim 6, further comprising a smart card having an encryption/decryption processor for encrypting/decrypting internal data, wherein the encryption/decryption processor performs the encryption/decryption using an encryption/decryption key according to a modular exponentiation operation, and the modular exponentiation operation is performed by the multiplier.